PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:	)	**Group Art Unit: 2134**
	)	
Wolfgang RANKL	)	**Examiner: M. Simitoski**
	)	
Serial Number: 09/492,273	)	***Attorney Docket*: RANK3001beu**
	)	
Filed: January 27, 2000	)	**Confirmation No.: 9676**

For: Method For Exchanging At Least One Secret Initial Value Between A Processing Station And A Chip Card

APPELLANT'S BRIEF UNDER 37 C.F.R. §1.192

Sir:

This paper is an Appeal Brief in furtherance of the Notice of Appeal filed in this case on April 20, 2005. The fee required under 37 C.F.R. §1.17(f) accompanies this Appeal Brief.

This Brief contains these items under the following headings and in the order set forth below:

I. Real Party In Interest

The real party in interest is Giesecke & Devrient, GmbH, of Munich, Germany.

II. Related Appeals And Interferences

There are no related appeals or interferences.

III. Status of Claims

The status of the claims in this application is:

A. Status of all the claims

1. Claims canceled: None
2. Claims withdrawn from consideration: None
3. Claims pending: 1-9
4. Claims allowed: None
5. Claims objected to: None
6. Claims rejected: 1-9

B. Claims on Appeal:

The claims on appeal are: 1-9

IV. Status of Amendments

No amendments have been submitted subsequent to the final rejection mailed February 2, 2005.

V. Summary of the Invention

The invention is a method of "initializing" a chip card (also known as a smart card, IC card, or integrated circuit card). The purpose of initialization is to store a secret value on the card, the secret value being used as, or to generate, encryption keys in order to protect and/or authenticate data on the card or communications between the card holder and a remote party.

Normally, chip cards are initialized by inserting the chip card into a processing station and then carrying out the initialization step by transferring the secret value (or values) to the chip card from the processing station. However, if the processing station is not in a secure location, the transfer may be intercepted and knowledge of the secret value used to comprise data communications involving the card. Therefore, the invention modifies the initialization step by substituting, for the conventional transfer of the secret value, an initialization step in which first and second values are generated by the processing station and circuitry on the chip card and only parts of the first and second values (represented in the Fig. as $X = g^x \bmod n$ and $Y = g^y \bmod n$) are transmitted. This procedure is known as a Diffie-Hellman key exchange.

Basically, the invention may be thought of as the application of a Diffie-Hellman key exchange to the establishment of a secret value on a chip card inserted into a processing station. Claim 1 recites the steps of inserting the chip card into the processing station, and initializing the chip card by:

> *having the processing station and the chip card each determine the secret initial value based on exchange of parts of first and second values generated, respectively, in the processing station and the chip card, wherein*
> - *first values for determining the secret initial value are generated in the processing station,*
> - *parts of the first values are transmitted to the chip card,*
> - *second values for determining the secret initial value are generated in the chip card,*
> - *parts of the second values are transmitted to the processing station,*
> - *the secret initial value is determined in the processing station from at least parts of the first values and the transmitted parts of the second values, and*
> - *the secret initial value is determined in the chip card from at least parts of the second values and the transmitted parts of the first values.*

The first and second values correspond to x and y shown in the Fig., while the "wherein. . ." clause recites the exchange of X and Y shown in the Fig., and the determination of the secret value K. Further aspects of the Diffie-Hellman exchange are recited in claims 3-5, while claim 7 recites use of the secret value as an encryption/decryption key.

Claim 2, on the other hand, recites the unique feature that at least one part of the second values is a serial number present on the chip card, while claims 6, 8, and 9 are directed to uses of the secret value during further card initialization steps, includes use of the secret value as a start value for generating random numbers (claim 6) and as a key for encryption/decryption of additional keys (claims 8 and 9), the key-encryption key being deleted subsequent to the establishment of the additional keys.

VI. Issues

The issues involved in this Appeal are:

1. whether the subject matter of claims 1, 3-5, and 7 is rendered obvious under 35 USC §103(a) by the subject matter disclosed in the publication entitled "*Applied Cryptography, Second Edition*" (Schneier) and U.S. Patent No. 5,602,918 (Chen);
2. whether the subject matter of claim 2 is rendered obvious under 35 USC §103(a) by the subject matter disclosed in the publications entitled "*Applied Cryptography, Second Edition*" (Schneier), "*Cryptographic Identification Methods For Smart Cards In The Process Of Standardization.*" (Konigs), "*Handbook of Applied Cryptography*" (Menezes), and U.S. Patent No. 5,602,918 (Chen);
3. whether the subject matter of claim 6 is rendered obvious under 35 USC §103(a) by the subject matter disclosed in the publication entitled "*Applied Cryptography, Second Edition*" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen) and 5,452,358 (Normile);
4. whether the subject matter of claim 8 is rendered obvious under 35 USC §103(a) by the subject matter disclosed in the publication entitled "*Applied Cryptography, Second Edition*" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen) and 6,038,551 (Barlow);
5. whether the subject matter of claims 9 is rendered obvious under 35 USC §103(a) by the subject matter disclosed in the publication entitled "*Applied Cryptography,*

Second Edition" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen), 6,038,551 (Barlow), and 5,224,163 (Gasser);

VII. Grouping of the Claims

Appellants most respectfully submit that claims 1, 3-5, and 7 may be grouped together, but that each of the remaining claims should be judged individually as they are the subject of separate rejections.

VIII. Arguments

1. Rejection of Claims 1, 3-5, and 7 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier) and U.S. Patent No. 5,602,918 (Chen)

Reversal of the rejection of claims 1, 3-5, and 7 is respectfully requested on the grounds that:

a. The Schneier article discloses three key exchange methods, none of which involves the claimed generation of first and second values ***by a processing station and a chip card inserted therein***, or the exchange of first and second values ***between the processing station and the chip card***. As will be explained in more detail below, the three methods include:

   (i) encryption of the keys by a previously initialized smart card, followed by key transfer;

   (ii) transfer of the entire key in parts over different channels; and

   (iii) Diffie-Hellman key generation corresponding to the claimed exchange of first and second values, but not in the context of a processing unit into which a chip card has been inserted.

b. The Chen patent describes a card initialization method in which secret values (*i.e.*, keys) are simply transferred from processor to card, in a physically secured location,

which is nothing more than the prior art discussed in the introductory portion of the present application.

The only mention of a smart card in the Schneier publication is in the last paragraph on page 176, which simply points that keys can be distributed using such a card. This passage does not specify how the card is initialized, *i.e.*, how the keys are placed on the card. The other key exchange teachings in Schneier do not mention smart cards. Instead, the method disclosed on page 7 involves transfer of parts of keys by such media as overnight delivery and carrier pigeon, while the Diffie-Hellman key exchange described on page 513 involves communications between separate parties, and not between a processing unit and a chip card. There is no suggestion in the Schneier publication of using Diffie-Hellman to initialize a chip card.

Initialization as used in the specification and claims of the instant application refers to the storage of numbers ("secret values") on a card for use in data encryption and/or key generation. In order to do this, it is conventional to simply transfer the keys to the card. The result is an initialized card that can subsequently be used to generate session keys, secured and/or authenticated communications, and to carry out data exchanges. The problem is that it might be possible to eavesdrop on the transfer of secret values to the card. The present invention solves this problem by using an algorithm that involves generation of first and second values by the processing station and by the card itself, and mutually transferring parts of the values thus generated for use in determining a secret initial value for the card and processing station.

On pages 176-177, the Schneier article describes two conventional options for transferring keys:

a. The first option uses "key-encrypting keys" to encrypt other keys for distribution. As explained in the last paragraph on page 176, "**These key-encrypting keys have**

to be distributed manually (although they can be secured in a tamperproof device, like a smart card). . . .." This passage describes an initialized card on which keys are provided, but does not describe how to initialize the card by providing the card with a key.

b. The second option shown in Fig. 2 on page 177 of the Schneier article, is to transfer keys by **splitting** them and transferring each of the parts of the key over a different channel. As explained on page 177, "One part could be sent over the **telephone**, one by **mail**, one by **overnight delivery service**, one by **carrier pigeon**, and so on." This passage not only does not describe card initialization, but the key transfer requires that all parts of the key be transferred (albeit by different media), which is not the case with the present invention. Because this method taught by Schneier requires multiple distribution channels, it is not suitable for card initialization (where only a single communications device, namely a card reader/writer, is used).

Even though the possibility of using a chip card is mentioned, neither of these key transfer options corresponds to the claimed invention.

On the other hand, the Diffie-Hellman algorithm described on pages 513-514 of the Schneier article corresponds to the method of secret value determination used by the claimed invention, but not as part of an initialization step. Instead, the key exchange is between a Bob and an Alice, which might be interpreted by those of ordinary skill in the art as two computers connected to an insecure network such as the Internet, but which is not suggestive of the claimed chip card inserted into a processing station.

The Examiner's response to the lack of teachings of the claimed step of "initializing the chip card by. . ." is to characterize the step an "intended use," arguing in item 5 on page 2 of the final Office Action, that

> *A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In a claim drawn to a process of making, the intended use must result in a manipulative difference as compared to the prior art. The Schneider reference merely discloses method steps. Without recitation in the claims of further method steps that occur either before or after the currently claimed steps, initialization is simply a use. Further, an invention can be initialized many times during its use. Absent further boundaries on the method steps, recitation that initialization is the purpose of the steps does not affect the method steps.*

Apparently, the Examiner's position is that:

- a method claim must involve **structural** differences to be patentable,
- a positively recited method step is an **intended use** if it is the first or last step in the claimed,
- the method step of intialization does not involve "**manipulation**," and
- the method step must for some reason be further limited in order to be a proper method step.

None of these reasons makes any sense, and while they represent a very creative attempt to avoid the need for teachings in the prior art, they are not in accord with the MPEP or court cases.

It is respectfully submitted that card initialization as recited in the body of claim 1 (as opposed to the preamble) is in fact a properly recited method step involving establishing secret values on a card inserted into a processing station, and that it is **not** an **intended use**. The step involves **manipulation** and transfer of first and second values. In the prior art, initialization normally consists of the actual physical transfer of the secret value to the card, while the present invention involves a modification of the prior art initialization step in which the secret value is established on the card (the card is "initialized") by transfers of parts of secret values that are

generated on the card and in the processing station, without transfer of either of the generated secret values.

The Examiner cites a number of court cases in support of the proposition that the positively recited step of "initialization" is an intended use rather than a method step, and that it may be ignored for the purpose of rejected the claimed based on prior art. These cases concern actual preamble limitations in apparatus claims and have nothing to do with the instant claims.

The first case is *In re Casey*, 152 USPQ 235 (CCPA 1967), which interprets a claim to "*A taping machine comprising a supporting structure, a brush attached to said supporting structure, said brush being formed with projecting bristles which terminate in free ends to collectively define a surface to which adhesive tape will detachably adhere. . .,*" and concludes that the preamble recitation of a taping machine did not distinguish a reference that showed exactly the same structure as positively recited in the body of the claim (*i.e.*, a brush with bristles to which tape will detachably adhere). Nowhere does this case suggest that it is permissible to ignore positively recited method steps (the step of "initializing") in a method claim for the purpose of applying prior art. To the contrary, the court specifically concluded that "*The claims in issue call for an apparatus or machine, viz. A tape dispensing machine. The manner or method in which such machine is to be utilized is not germane to the issue of patentability of the machine itself.*" Clearly, the court's conclusion that a preamble method limitation is not germane to the patentability of a claim to a **machine** is irrelevant to the instant **method** claim.

The second case, *In re Otto*, 136 USPQ 458, is equally irrelevant. The *Otto* case involved both an apparatus claim (to a hair curler core) and a method claim (to a method of making a hair curler core). The court concluded that the manner of intended use recited in the preamble of the

apparatus claim was of no significance, *and further that the feature (involving attachment of hair) was obvious*. As to the method claim, the court concluded:

> Coming to claim 4, the only aspect of the recited method which requires additional consideration reads: ***, saturation the body with a hair waving lotion *** and thereafter permitting the saturated body to dry, *** adapted to be activated by subsequent wetting of the body.
> It does not appear to us that it would be beyond the skill of an ordinary workman in this art who desires to impregnate a foam-like material with a liquid soluble substance to prepare that substance in liquid form then saturate the material with it. . .We feel certain that this procedure takes place every day in the homes in this country where a housewife saturate a sponge with soapy water then permits the sponge to dry, . . .

Again, nothing in this case suggests that a method step in a method claim can be ignored by characterizing the method step as an intended use. The case discusses intended use limitations, but only with respect to the **preamble** of an **apparatus claim**. The limitation in question in the present case is **not in the preamble** and not part of an **apparatus claim**. In the *Otto* case, the court did not ignore any limitations in the method claim or characterize them as intended uses. Instead, it dealt with the steps of the method claim on the merits.

Claim 1 of the present application specifically and positively recites two method steps:

- "**inserting** a chip card into a processing station"; and
- "**initializing** the chip card by having the **processing station** and the **chip card** each determine the secret initial value based on exchange of parts of first and second values generated, respectively, in the processing station and the chip card. . .."

The chip card **initialization** step is further limited by the following conditions related to the functions carried out by the processing station and the chip card:

- first values for determining the secret initial value are generated in the processing station,
- parts of the first values are transmitted to the chip card,
- second values for determining the secret initial value are generated in the chip card,

- parts of the second values are transmitted to the processing station,
- the secret initial value is determined in the processing station from at least parts of the first values and the transmitted parts of the second values, and
- the secret initial value is determined in the chip card from at least parts of the second values and the transmitted parts of the first values

The Schneier article does not disclose a card initialization step, much less a card initialization step that involves transmission of only parts of first and second values in the manner claimed, and therefore the Schneier patent cannot overcome the teachings of Chen that card initialization should be carried out by simplify storing secret values on the card.

Of the applied references, only the Chen patent even mentions card initialization. However, like the prior art described on pages 1 and 2 of the specification, the Chen patent requires the initialization to be performed at a "***physically secure location***" (col. 4, line 6). This is because, in order to prepare the card to perform DES encryption, as disclosed by Chen, the DES key must be transferred to the card. Since the card has not previously been provided with keys, the transfer is carried out by means of plain text. That is the reason that a "physically secure location" is required. **If Chen had found a way to modify the Diffie-Hellman algorithm taught by Schneier so as to enable initialize the card, then a "*physically secure location*" would not have been required.** Therefore, one of ordinary skill in the art familiar with the Chen patent would not have thought to apply the teachings of Schneier concern key distribution using Diffie-Hellman (or the smart card and key splitting methods mentioned on pages 176 and 177).

The Examiner responds to this in item 5 of the Official Action by arguing that "*Chen is relied upon for teaching that smart cards need to be initialized (col. 4, lines 5-31),*" and not for its teaching of simply transferring the keys to the chip card. It is respectfully submitted that the Examiner, in ignoring what Chen actually teaches about card initialization, is clearly engaging in hindsight reconstruction of the references. Such selection of isolated teachings rather than consideration of

the reference "as a whole," is clearly improper. For example, *In re Gorman,* 18 USPQ 2d 1886, 1888 (Fed. Cir. 1990) points out that it is improper

> *...simply to engage in a hindsight reconstruction of the claim invention, using the applicant's structure as a template and selecting elements from references to fill the gaps* [citing *Interconnect Planning Corporation v. Feil*, 227 USPQ 543, 551 (Fed. Cir. 1985)].

What the Chen patent actually teaches is that in order to initialize a card, it is necessary to transfer secret values (or keys) to the card. This is exactly the problem that the present invention seeks to solve. To ignore that Chen teaches an alternative and contrary intialization method is precisely the type of templating mentioned in the *Gorman* case. See, also, MPEP 2141.02, p. 2100-107: "a prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention" (emphasis in the original). If the Applicant had claimed the broad concept of initialization, then it would be proper to ignore the details of the method taught by Chen. However, the Applicant did not claim to have invented the broad concept of initialization, but rather has invented an improved to the conventional initialization method, and therefore the fact that Chen teaches a contrary method is relevant to the determination of patentability.

Because neither the Schneier article nor the Chen patent discloses or suggests the claimed chip card ***initialization*** method in which only parts of values that are used to generate secret values are exchanged, it is respectfully submitted that the Schneier article and the Chen patent, whether considered individually or in any reasonable combination, could not possible have suggested the claimed invention, and withdrawal of the rejection of claims 1, 3-5, and 7 under 35 USC §103(a) is respectfully requested.

2. Rejection of Claim 2 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier), "Cryptographic Identification Methods..." (Konigs), "Handbook of Applied Cryptography" (Menezes), and U.S. Patent No. 5,602,918 (Chen)

This rejection should be reversed on the grounds that the Konigs and Menezes articles, like the Schneier article and the Chen patent, fails to disclose or suggest a chip card **initialization** step in which the second value used in the Diffie-Hellman exchange is the serial number of the card.

Instead, the Konigs article discloses a method of establishing cryptographic data connections using chip cards without containing any suggestion as to how the chip cards used for the cryptographic data connections are initialized for use in the cryptographic connections, while the Menezes publication merely teaches the use of sequence numbers to identify entities in key establishment protocols, and does not teach any specific initialization method of the type claimed.

The passage on page 46 of the Konigs article cited by the Examiner as teaching use of a serial number as the second value of the Diffie-Hellman key exchange contains no such teaching, but rather states that "*alternatives* [to a public key authentication] *are also possible in which the verification key can be deduced from the identification word (unique short name) of the prover.*" In other words, Konigs simply teaches that authentication can be carried out by adding a card identifier. According to Konigs, while such methods "*greatly simplify the problem o key management,*" they also have the disadvantage that "*these techniques require centralized preparation of the secret identification characteristics, e.g., centralized smart card personalization,*" *i.e.*, initialization.

Since Konigs cites the need for initialization as a disadvantage, it may reasonably assumed that this passage does not teach the use of the identifier to facilitate initialization by serving as the "second value" in a Diffie-Hellman key exchange. As a result, reversal of the rejection of claim 2 under 35 USC §103(a) is respectfully requested

3. Rejection of Claim 6 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen) and 5,452,358 (Normile)

Reversal of this rejection is respectfully requested on the grounds that the Normile patent, like the the Schneier article and the Chen patent, fails to disclose or suggest a chip card **initialization** step in which secret initial values are generated both at the card and at the processing station in the manner claimed, by exchange of values used to generate the secret values without actual exchange of any part of the secret initial values.

Instead, the Normile patent merely discloses public key encryption of a plaintext message. The public key of a private-public key pair can by definition be exchanged in public, and therefore there is no need to use parallel key generation. The private key, on the other hand, is maintained by only one party, and again there is no need for the claimed type of card initialization, which is useful for shared-secret key initialization but not for public-private key pair generation.

Because the Normile patent basically has nothing to do with the claimed invention, reversal of the rejection of claim 8 under 35 USC §103(a) in view of the Schneier article and the Chen and Normile patents is respectfully requested.

4. Rejection of Claim 8 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen) and 6,038,551 (Barlow)

Reversal of this rejection is respectfully requested on the grounds that neither the Schneier article nor the Chen patent, whether considered individually or in any reasonable combination, discloses or suggests a chip card **initialization** step that does not involve exchange of any part of secret values generated during the initialization.

Instead, the Barlow patent teaches a system that not only exchanges secret keys, but does so by means of public key encryption of the exchanged secret keys. This is the key encryption method

discussed by Schneier. Barlow makes no attempt to only exchange parts of secret values, but rather simply encrypts all of the values before exchange (col. 3, lines 1-13). This public key method of Barlow is not suitable for chip card initialization since chip card initialization begins with a blank card and not one that already includes a public decryption key, and Barlow does not even remotely suggest a method of generating an initialization value without exchanging the values.

To the contrary, whereas the claimed invention is capable of generating initial values for each chip card manufactured in a relatively simple and yet secure manner, Barlow teaches the difficulty of providing millions of different devices with individual keys, and instead suggests providing them all with a common *public* key. This essentially ***teaches away*** from the claimed invention since it implies that each stored key must in fact be encrypted by an individual data key, *or* a common public key must be used. Use of a common public key means that the data on the card is either first encrypted and then transferred to the card, or that an encryption key has already been provided on the card, in which case the card is not being initialized..

In item 11 on page 4 of the Official Action, the Examiner argues that Barlow does not teach away from the claimed invention because Barlow is cited for its teaching of multiple keys, and not for its teaching that a public key needs to be used to protect keys stored on the card. Apparently, the Examiner believes that by not citing the portions of the reference that teach away from the claimed invention, the teaching away is negated. This argument clearly involves precisely the type of templating prohibited by the above-cited "as a whole" rule.

In addition, the Examiner refers to Schneier's teaching of key-encryption keys. As noted above, this teaching is but one of several alternative key distribution methods taught by Schneier, and is not relevant to the claimed invention which does not seek to encrypt any keys for distribution.

Consequently, reversal of the rejection of claim 8 under 35 USC §103(a) in view of the Schneier article and the Chen and Barlow patents is respectfully requested.

5. Rejection of Claim 9 Under 35 USC §103(a) in view of "Applied Cryptography, Second Edition" (Schneier) and U.S. Patent Nos. 5,602,918 (Chen), 6,038,551 (Barlow), and 5,224,163 (Gasser)

Reversal of this rejection is respectfully requested on the grounds that the Gasser patent, like the Chen and Barlow patents, fails to disclose a card **initialization** step in which transfer of data to the card is facilitated by a "secret value" exchange that involves transfer only of "parts" of the respective secret values, as claimed.

Instead, the Gasser patent disclose generation of "session public/private encryption key pairs." The session public/private key pairs are generated, as is common in such session key generating schemes, by mutual exchange and processing of secret values, but there is **no disclosure** in the Gasser patent that the secret values used in the public/private session key generating process may be transferred to the chip card by a secret value generated in the manner claimed, using parts of two values respectively generated in the chip card and the processing unit.

Accordingly, reversal of the rejection of claim 9 under 35 USC §103(a) in view of the Schneier article and the Chen, Barlow, and Gasser patents is respectfully requested.

IX. Conclusion

For all of the foregoing reasons, Appellants respectfully submit that the Examiner's final rejections of claims 1-9 under 35 U.S.C. §103(a) are improper and should be reversed by this Honorable Board.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: April 20, 2005

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

S:\Producer\beu\Pending Q...Z\R\RANKL 492273\Appeal Brief.wpd

X. APPENDIX OF CLAIMS

1. A method of initializing a chip card, comprising the steps of:

inserting a chip card into a processing station, and

initializing the chip card by having the processing station and ~~a~~ the chip card each determine the secret initial value based on exchange of parts of first and second values generated, respectively, in the processing station and the chip card, wherein

- first values for determining the secret initial value are generated in the processing station,
- parts of the first values are transmitted to the chip card,
- second values for determining the secret initial value are generated in the chip card,
- parts of the second values are transmitted to the processing station,
- the secret initial value is determined in the processing station from at least parts of the first values and the transmitted parts of the second values, and
- the secret initial value is determined in the chip card from at least parts of the second values and the transmitted parts of the first values.

2. A method according to claim 1, characterized in that at least one part of the second values generated in the chip card is generated in accordance with a serial number present in the chip card.

3. A method according to claim 1, characterized in that

- the first values generated in the processing station are subjected to a first function,
- the result of the first function is transmitted to the chip card in addition to the part of the first values generated,
- at least one part of the second values generated in the chip card is subjected to a second function with the transmitted part of the first values,

- the secret initial value is generated in the processing station by means of a third function from the transmitted result of the second function and a part of the first values, in particular the first part of the values not transmitted to the chip card, and
- the secret initial value is generated in the chip card by means of a fourth function from the transmitted result of the first function, the transmitted part of the first values and a part of the second values not transmitted to the processing station,

4. A method according to claim 3, characterized in that the first, second, third and fourth functions are identical.

5. A method according to claim 4, characterized in that the function involves exponentiating a first variable with a second variable and forming a modulo residue to a third variable, the variables corresponding to the first and second values and the first and second results.

6. A method according to claim 1, characterized in that the secret initial value is a start value for generating random numbers.

7. A method according to claim 1, characterized in that the secret initial value is a key for encrypting and decrypting data.

8. A method according to claim 7, characterized in that the key generated in the processing station and the chip card is used in a personalizing step for encrypting and decrypting further secret keys, which are transmitted from the processing station to the chip card.

9. A method according to claim 8, characterized in that the key generated in the processing station and the chip card is deleted in the processing station and the chip card after the personalizing step.